

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Case No. 1:20-CR-143
v.	)	
	)	Honorable T.S. Ellis, III
ZACKARY ELLIS SANDERS,	)	
	)	Trial: April 26, 2021
<i>Defendant.</i>	)	
_____	)	

**GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT'S  
MOTION TO MODIFY THE PROTECTIVE ORDER**

The defendant has moved to modify the agreed-upon Protective Order now that discovery has been provided so he can disseminate sensitive material and sealed filings in this case to individuals who are not part of the defense team. Dkt. No. 229. The United States, by and through its undersigned counsel, hereby files this response in opposition to the defendant's motion.

The government has produced substantial discovery in this case pursuant to the agreed-upon Protective Order, which permits the defendant to share copies of this material with a broadly defined defense team consisting of lawyers, investigators, experts, and others. Dkt. No. 28. Since receiving discovery, the defendant has done just that, sharing this sensitive material with others on his team—including multiple academics, another lawyer who is not counsel of record, and a computer privacy specialist recently employed by a non-profit internet privacy organization—while preparing pre-trial motions. Dissatisfied with the outcome of these motions, the defendant now seeks to modify the Protective Order so he can widely share sensitive material and sealed documents to unidentified individuals who are not a part of this case and enlist them in his ongoing fishing expedition for immaterial information to support his failed suppression arguments. The information he purports to seek through his proposed modifications, however, has already been

provided to him through discovery and litigation in this case, and it is all immaterial. Further, these proposed modifications would render the Protective Order unenforceable. Given that the material he seeks to circulate to others pertains to sensitive, ongoing investigations in the United States, the defendant's motion should be denied.

### **BACKGROUND**

On June 24, 2020, a federal grand jury returned a twelve-count indictment charging the defendant with production, receipt, and possession of child pornography. Dkt. No. 29. The charges in this case stem from evidence obtained during a February 12, 2020, search of his home pursuant to a warrant issued by Magistrate Judge John F. Anderson. Dkt. No. 86, Ex. 11. The affidavit in support of the warrant is based in part on a tip from a foreign law enforcement agency ("FLA") that the defendant's Internet Protocol ("IP") address had been used to access child sexual abuse material on a hidden service ("Target Website") on The Onion Router ("Tor"). Dkt. No. 86, Ex. 5 at ¶¶ 23–25. While the defendant has now been arrested and charged with various child-pornography crimes, the United States continues to investigate other individuals based on IP address information provided by the FLA. *Id.* at ¶ 6 n.1. Accordingly, and for the reasons explained in other submissions and incorporated here, *see* Dkt. Nos. 121, 173, and 193, certain details about the Target Website and the FLA's investigation remain sensitive.

In order to produce sensitive discovery prior to the defendant's indictment, the government filed a motion with the express consent of the defendant for the entry of a Protective Order on April 27, 2020. Dkt. No. 27. That same day, the Court entered the Protective Order, signed and agreed to by counsel for the government and defense counsel. Dkt. No. 28. The Protective Order governs all discovery produced by the government in this matter and any information contained therein. *Id.* at 1. It limits the possession of copies of discovery materials to the defense team,

broadly defined as “the attorneys of record, and investigators, paralegals, law clerks, experts, and assistants for the attorneys of record[.]” *Id.* It also instructs that the defense team shall “use discovery only for the preparation and litigation of this matter,” which includes pre-trial, trial, and post-trial and appellate proceedings, “and for no other purpose.” *Id.* at 2–3.

After the government provided the defendant with the search warrant materials and related discovery pursuant to the Protective Order, the defense retained several purported experts and provided them with this material to assist with the defendant’s motions to compel discovery and suppress evidence. These experts include: (1) a professor of computer science, *see* Dkt. No. 38, Ex. 1; (2) a computer privacy specialist who was recently employed by a non-profit computer privacy organization, Dkt. No. 84, Ex. 7; (3) a research associate who focuses on cybercrime and internet tracing, Dkt. No. 84, Ex. 8; and (4) an attorney who is not counsel of record in this case, Dkt. No. 91, Ex. 7. Following extensive briefing and arguments, the Court denied the defendant’s first motion to compel, Dkt. No. 74, his motion for reconsideration of his motion to compel, Dkt. No. 107, and his four motions to suppress, Dkt. No. 114. Consistent with the Court’s instructions, the government has moved to publicly file versions of the Court’s rulings on these motions that redact only the most sensitive information. Dkt. Nos. 120 and 144.

On November 27, 2020, the defendant filed a renewed motion for reconsideration of his prior motion to compel. Dkt. No. 135. While that motion was pending, the defendant also filed the instant motion to modify the Protective Order, arguing that the modifications will allow him to obtain evidence he has been denied to support his prior suppression claims. Dkt. No. 230. On January 26, 2021, the Court denied the defendant’s renewed motion for reconsideration of his motion to compel, explaining that the defendant had failed to establish the materiality of the requested information. Dkt. No. 237. In particular, the Court found that the defendant’s repetitive,

unsupported claim that his IP address was only used to access the homepage of the Target Website and not any illegal content “misse[d] the point entirely.” *Id.* at 2 n.1. As the Court explained, the FLA’s tip states that his IP address was used to access child sexual abuse material and not just the homepage, which the affidavit in support of the search warrant accurately conveyed. *Id.* And even if the FLA’s tip intended to convey that the defendant only accessed the website’s homepage, the Court found that the multiple affirmative steps a user would need to take to do so “warrants the inference” that the user did so intentionally to access the child sexual abuse material on the Target Website, which is sufficient to establish probable cause to search the defendant’s home. *Id.*

### **ARGUMENT**

The defendant argues that the agreed-upon Protective Order should be significantly altered now that the government has provided discovery so he can disseminate this sensitive information and the sealed filings in this case to any defense teams representing clients who he believes have been charged based on the FLA’s investigation and any public interest organizations.<sup>1</sup> Dkt. No. 230 at 3–4. He asserts that these modifications are necessary so that he can re-litigate his failed claims regarding the search warrant—namely, his belief that the FLA’s tip was not specific to him and, to the extent it was, that it was also false. *Id.* at 7. And while he assumes that the discovery he received is no longer sensitive, he also claims with little explanation that distributing discovery materials and sealed filings in this case to a vaguely defined group of third parties will not jeopardize any ongoing investigations because these third parties will follow the Court’s Protective Order. *Id.* at 3–5, 8–10.

---

<sup>1</sup> While the defendant suggests that he will send this sensitive discovery to undefined “public interest organizations” that may file amicus briefs or expert affidavits, the proposed modifications do not limit the organizations’ use of this sensitive discovery to this case or even to the preparation of such documents. Dkt. No. 229 at 4–5.

These arguments lack merit. The continued maintenance of the Protective Order is supported by good cause because the investigation into other users who accessed child sexual abuse material on the Target Website is ongoing and the disclosure of protected information in this case could alert the targets of these ongoing investigations and provide them with an opportunity to destroy evidence or flee. Further, the defendant already has much of the information he claims he can only obtain by vitiating the agreed-upon Protective Order, and none of it has any bearing on his ability to prepare for trial. He is of course free to add individuals to his defense team to review this discovery—as he has already done—but he provides no plausible explanation how the Protective Order has materially impacted his ability to defend himself in this case, particularly since the government has already moved to unseal all but a handful of sensitive details from the Court’s prior rulings. Accordingly, his motion should be denied.

**I. Good Cause Exists to Maintain the Protective Order Because the Discovery Materials Contain Sensitive Information Relevant to Ongoing Investigations**

Federal Rule of Criminal Procedure 16 provides courts with broad discretion to oversee the criminal discovery process, including by entering protective orders “for good cause [that] deny, restrict, or defer discovery or inspection, or grant other appropriate relief.” Fed. R. Crim. P. 16(d). As another court recently explained, courts across the country “have applied the standard for modification of protective orders in the civil context to the criminal context,” and, “[i]n the civil context, there is a strong presumption against the modification of a protective order.” *United States v. Maxwell*, 20-cr-330 (AJN), 2020 WL 5237334, at \*1 n.2 (S.D.N.Y. Sept. 2, 2020) (internal citations and quotation marks omitted); *see also United States v. Kerik*, 07-cr-1027 (LAP), 2014 WL 12710346, at \*1 (S.D.N.Y. July 23, 2014) (“[T]here is a general and strong presumption against access to documents sealed under protective order when there was reasonable reliance upon such an order and it is presumptively unfair for courts to modify protective orders which assure

confidentiality and upon which the parties have reasonably relied.” (internal citation and quotation marks omitted)); *United States v. Morales*, 807 F.3d 717, 723 (5th Cir. 2015) (using civil “good cause” standard to evaluate modification of criminal protective order); *United States v. Wecht*, 484 F.3d 194, 211 (3rd Cir. 2007) (same). Ultimately, however, Rule 16 gives courts broad authority “to limit [the disclosure of discovery], condition it, or absolutely prohibit it in the interests of witness security or any other compelling reason[.]” *United States v. Roberts*, 793 F.2d 580, 587 (4th Cir. 1986), *vacated on other grounds*, 811 F.2d 257 (4th Cir. 1987).

Here, good cause exists to maintain the current Protective Order because the investigation of other users besides the defendant who accessed child sexual abuse material on the Target Website remains ongoing and the protected discovery contains details regarding those investigations. This includes information that could be used to identify the Target Website, which, if made public, would alert other targets who accessed such material on the site that they may be under investigation and provide them with an opportunity to destroy evidence or flee.<sup>2</sup> Those concerns are heightened where, as here, law enforcement is investigating targets engaged in the sexual exploitation of children and the disclosure of the sensitive discovery would hinder law enforcement’s efforts to identify offenders and rescue children from further abuse (as was the case with the defendant, who had been sexually exploiting minors for several years and whose conduct was discovered only upon searching his home pursuant to the FLA’s tip). Multiple courts have found good cause to grant protective orders in similar circumstances. *See, e.g., United States v. Jones*, No. CR-20-00634, 2021 WL 24585, at \*1 (D. Ariz. Jan. 4, 2021) (noting that protective orders “in criminal cases are not uncommon,” particularly “where discovery material reveals

---

<sup>2</sup> The defendant’s speculation that it is “not plausible” this information remains sensitive given the amount of time that has elapsed since the FLA provided the tip about his IP address, Dkt. No. 230 at 4, is therefore incorrect.

details, sources, and methods of ongoing law enforcement investigations”); *United States v. Chow*, No. CR 14-00196, 2014 WL 2093488, at \*1 (N.D. Cal. May 19, 2014) (granting motion for entry of order to protect “sensitive materials that, if improperly disclosed, could be used to identify individuals who have not yet been charged by the United States, but whose ongoing criminal activities are still under investigation”); *United States v. Smith*, 985 F. Supp. 2d 506, 530 (S.D.N.Y. 2013) (“Thus, where public disclosure of certain materials might officially reveal the sources and methods law-enforcement officials have used, and will continue to use, to investigate other criminal conduct related to the publicly filed charges, courts have found it appropriate to enter a protective order.” (citations omitted)).

Further, and contrary to the defendant’s suggestions, Dkt. No. 230 at 8–9, the protected discovery in this case contains sensitive information about the FLA’s investigation that is not publicly known, and the FLA requested that this material remain protected to the greatest extent possible. While the defendant argues that this information is effectively public because of an assortment of articles and documents he found online, these documents—several of which are years old and not related to this investigation at all—are vague and generally meaningless unless viewed in connection with the sensitive information provided in this case pursuant to the Protective Order. As an extension of this argument, the defendant also asserts that the Protective Order should be modified so as not to cover any information he found online or through other sources. Dkt. No. 230 at 4. But as he demonstrated in the civil complaint he filed in an adjacent district, the defendant would rely on this modification to publicly link these otherwise unrelated articles and documents to the information contained in the filings in this case, which would reveal the exact information the government seeks to protect. *See* Dkt. No. 173-1. And as this Court already observed, he can only make these numerous “logical connections between sparsely detailed information” because

of the sensitive discovery in this case. Dkt. No. 228 at 2. The defendant's proposed modifications to the Protective Order would therefore jeopardize ongoing and future investigations by inviting others, including the potential targets of the investigations, to make these same connections. *Id.*

Finally, the defendant claims that the proposed modifications would not jeopardize any ongoing or future investigations because the various third parties to whom he intends to circulate sensitive materials will follow this Court's Order. Dkt. No. 229 at 5; Dkt. No. 230 at 8. Despite his un-evidenced assurances, the defendant's proposed modifications would eviscerate the Protective Order. The proposed modifications do not: identify who these third parties are; require the defendant to disclose who they are; or limit the third parties' use of this sensitive information to filings in this case. Neither the United States nor the Court would have any practical way to determine whether these third parties are disseminating this information to others or publicly disclosing sensitive details of the investigation. And even if the government found out that another defense team or a public interest organization publicly disclosed sensitive information, it is unclear what recourse the government would have over an individual or entity who is not a party to this case. To the extent that this Court has the authority to instruct a non-party to this case to take down such information, the process would undoubtedly be time-consuming and public. After all, when the defendant himself publicly filed sensitive, protected details about this investigation on the docket in an adjacent district, those details remained improperly in public view for approximately 39 days while the government sought and obtained relief from the Court. The public dissemination of sensitive investigative details by others could easily go unnoticed and un-remedied for far longer, if ever remedied at all.

Despite these sensitivities, the government has moved to unseal large portions of the Court's prior rulings. The redacted information in these rulings and the sensitive details in the



discovery provided pursuant to the Protective Order, however, remain sensitive for the reasons above. Accordingly, the government submits that good cause exists for maintaining the continued operation of the Protective Order without modification.

## **II. The Defendant Provides No Plausible Explanation How the Protective Order is Limiting his Defense**

The defendant also argues that the Protective Order should be modified because it is “preventing [him] from mounting an effective defense” with respect to his failed challenges to the search warrant in this case. Dkt. No. 230 at 5. Specifically, he asserts that the proposed modifications will allow him to: (1) confirm the “scope of the operation and the FBI’s use of a template affidavit”; (2) “demonstrate that this was a large-scale operation involving many Internet users”; and (3) somehow show that his IP address was only used to access the homepage of the Target Website. Dkt. No. 230 at 5–8. Put simply, this information is either immaterial or already known to him, and there is no plausible claim that the Protective Order is limiting his defense.

As an initial matter, the defendant’s repeated claim that his IP address was only used to access the homepage of the Target Website is wishful speculation on his part that “misses the point entirely.” Dkt. No. 237 at 2 n.1. As this Court has repeatedly found, the FLA’s tip states that his IP address was used to access child sexual abuse material on the Target Website, not its homepage, and the affidavit in support of the search warrant accurately conveys that fact. Dkt. No. 73 at 10–11; Dkt. No. 107 at 5–6; Dkt. No. 113 at 12–13; and Dkt. No. 237 at 2 n.1. There is no basis to support his theory of the tip beyond his own repeated incantation. Further, his claim that permitting him to widely share sensitive discovery in this case with third parties will somehow uncover information supporting his theory of what his IP address accessed is implausible. Even assuming that an unknown third party is somehow in possession of information proving that the defendant’s IP address was only used to access the Target Website’s homepage—which is, to be clear, baseless

speculation—that information would not prove that his Fourth Amendment rights were violated. As this Court has repeatedly found, the affidavit in support of the search warrant establishes that navigating to the Target Website requires multiple affirmative steps, which “clearly invites and warrants the reasonable inference that the IP address user was purposeful in his efforts to reach the [Target Website] and its illegal content.” Dkt. No. 113 at 13; *see also* Dkt. No. 237 at 2 n.1. That is sufficient to conclude that there was a fair probability of finding contraband—that is, child sexual abuse material—at the defendant’s residence, as required to establish probable cause for the search. Dkt. No. 113 at 13.

The defendant’s remaining claims as to how the Protective Order is limiting his ability to defend himself are equally unavailing. For example, he claims that the Protective Order in its current state is preventing him from arguing that his prosecution stems from a large-scale operation involving multiple internet users, Dkt. No. 230 at 5–7, despite making this exact argument in one of his motions to suppress, Dkt. No. 86 at 28–29. He also claims that the government sought to conceal the scope of this investigation from the Court. Dkt. No. 230 at 7. That claim is based on a pedantic reading of cherry-picked language from the government’s filings and is belied by the record as a whole. While the FLA provided the FBI with one tip related to the defendant’s IP address, the government’s discovery and pleadings in this case have repeatedly made it obvious that its investigation extends beyond just this defendant’s illegal activity on Tor. That information is disclosed in: the search warrant affidavit, Dkt. No. 86, Ex. 5 at ¶ 6 n.1 (“Investigation into the users of the [Target Website] remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.”), *see also id.* at ¶¶ 22, 26; the affidavit in support of the criminal complaint, Dkt. No. 4 at ¶ 9 (“The FBI, in conjunction with

other law enforcement entities, is investigating websites on which visitors can access and view child sexual abuse material.”); the government’s response to the defendant’s four motions to suppress, Dkt. No. 97 at 18 (“[T]he Affidavit specifically noted that the FLA provided tips about other IP addresses that led to the apprehension of child sex offenders . . . ”); and, perhaps most obviously, the FLA’s tip, Dkt. No. 86, Ex. 2 (“The [FLA has] provided data to the United States Federal Bureau of Investigation in relation to Internet addresses (IPs), associated to individuals who have accessed online Child Sexual Abuse and Exploitation material[.]”).

Moreover, the obvious scope of the government’s investigation is immaterial to the defendant’s case. The fact that the FLA identified other users who accessed child sexual abuse material on Tor has no bearing on its tip with respect to the defendant’s IP address, which the search warrant affidavit accurately describes. He has not been charged in a conspiracy with any of these other users and is therefore not entitled to any discovery related to them. And, as noted above, the search warrant affidavit states that the government is investigating other users of the Target Website. There is therefore no plausible claim that the affidavit was misleading—let alone materially so—with respect to the scope of the government’s investigation, nor that the scope of this investigation provides a basis to question the conclusion of this Court and Magistrate Judge Anderson that the affidavit established probable cause to search the defendant’s home. The defendant’s speculation regarding the possibility of a “template affidavit” is similarly immaterial. The validity of the warrant turns on the information contained in the affidavit presented to Magistrate Judge Anderson, not other affidavits in support of warrants to search other homes in other cases. This Court has already found that the affidavit here establishes probable cause to search his home and that its description of the FLA’s specific tip regarding the defendant’s IP address and the Target Website is not misleading in any material respect. Dkt. No. 113. The

Protective Order is therefore not preventing the defendant from “investigat[ing] . . . whether his Fourth Amendment rights were violated” because the information he claims to need is either immaterial, already clear based on the pleadings and discovery, or both.

More fundamentally, the defendant fails to articulate how the Protective Order is preventing him from receiving effective counsel or preventing his counsel from investigating the circumstances of his case. He has received discovery from the government, thoroughly reviewed and researched this material, hired multiple experts to assist in his defense, and repeatedly used the available legal procedures to seek additional discovery and suppress the evidence against him. That is what is contemplated in the cases and rules the defendant cites in his motion. Dkt. No. 230 at 6. He cites no authority for his suggestion that his counsel should be permitted to widely disseminate discovery materials to all interested third parties as part of his defense, particularly when the materials pertain to sensitive, ongoing investigations related to the sexual abuse of children. He also fails to explain how modifying the Protective Order is necessary when the government has already moved to unseal large portions of the Court’s prior rulings that reveal significant information about this investigation. While sensitive from a law enforcement perspective, information that specifically identifies the Target Website or the FLA’s investigation is largely irrelevant to a third party seeking to prepare an amicus brief or affidavit given the significant amount of information in the Court’s public rulings. And, finally, the defendant fails to address that the Protective Order permits him to share sensitive discovery with any other lawyers, experts, or investigators on his defense team, which he has already done on multiple occasions.

This is because, at base, the Protective Order is not limiting the defendant’s ability to “investigate” whether his Fourth Amendment rights were violated. Dkt. No. 230 at 6–7. It is

limiting his ability to fish for immaterial and irrelevant information to use to re-litigate his failed motions. He has, at this point, filed three motions seeking to compel the government to produce wide-ranging and unspecified materials so he can search for any information to support his otherwise baseless challenges to the valid search warrant in this case. The government has repeatedly explained that the information he seeks is not material, and the Court has agreed. He now seeks to vitiate the agreed-upon Protective Order to work around the Court's rulings and recruit others to join him in this fishing expedition. But, as set forth above, good cause exists to maintain the Protective Order in this case without modification and the defendant remains free to add any other experts, investigators, or lawyers to his defense team to review the sensitive discovery in this case. Accordingly, his motion should be denied.

### **CONCLUSION**

For the foregoing reasons, the government respectfully requests that the Court deny the defendant's motion to modify the Protective Order. Dkt. No. 229.

Respectfully submitted,

Raj Parekh  
Acting United States Attorney

By: \_\_\_\_\_/s/\_\_\_\_\_  
William G. Clayman  
Special Assistant United States Attorney (LT)  
Jay V. Prabhu  
Assistant United States Attorney  
United States Attorney's Office  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
Phone: 703-299-3700  
Fax: 703-299-3981  
Email: william.g.clayman@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on February 3, 2021, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which automatically generated a Notice of Electronic Filing to the parties of record.

By: \_\_\_\_\_/s/\_\_\_\_\_  
William G. Clayman  
Special Assistant United States Attorney (LT)  
United States Attorney's Office  
Eastern District of Virginia  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
(703) 299-3700  
Email: [william.g.clayman@usdoj.gov](mailto:william.g.clayman@usdoj.gov)